Directed Association Mechanism in Wireless Network Environments

CROSS-REFERENCE TO RELATED APPLICATIONS

This application makes reference to the following commonly owned U.S. patent applications and patents, which are incorporated herein by reference in their entirety for all purposes:

U.S. patent application Ser. No. 10/155,938 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN;"

U.S. patent application Ser. No. 10/407,357 in the name of Patrice R. Calhoun, Robert B. O'Hara, Jr. and Robert J. Friday, entitled "Method and System for Hierarchical Processing of Protocol Information in a Wireless LAN;"

U.S. patent application Ser. No. 10/407,370 in the name of Paul Dietrich, Robert B. O'Hara, Jr. and David A. Frascone, entitled "Wireless Network System Including Rogue Access Point Detection;"

U.S. patent application Ser. No. 10/409,246 in the name of Robert J. Friday and Alexander H. Hills, entitled "Method And System For Dynamically Assigning Network Resources In Wireless Network;" and

U.S. patent application Ser. No. 10/447,735 in the name of Robert B. O'Hara, Jr., Robert J. Friday, Patrice R. Calhoun and Paul Dietrich, entitled "Wireless Network Infrastructure including Wireless Discovery and Communication Mechanism."

FIELD OF THE INVENTION

The present invention relates to wireless computer networks and, more particularly, to methods, apparatuses and systems enabling a directed association mechanism in wireless computer network environments.

BACKGROUND OF THE INVENTION

Wireless computer network environments generally comprise a plurality of wireless access points that, when operating in the infrastructure mode, bridge wireless traffic between a wired computer network and the wireless clients that associate with the access points. A wireless Local Area Network (WLAN) is a wireless communication system with radios having relatively high throughput and short coverage ranges. Many wireless LANs are based on iterations of the IEEE 802.11 standard. When a wireless client initializes or moves into an entirely new coverage area, according to the 802.11 standard, it transmits probe requests to locate access points to which it may associate to establish a wireless connection. Often, the wireless client may detect multiple access points. The 802.11 standard, however, generally leaves it to the wireless client to decide with which access point to associate. That is, a wireless client scans the available channels in the region and listens to the Beacon or Probe Response Frames transmitted by access points in that region. The wireless client stores the RSSI (Received Signal Strength Indicator) of the Beacon or Probe Response Frames and other relevant information, such as BSSID, encryption (on/off), etc. After finishing the scanning procedure, the wireless client generally selects the access point with the maximum RSSI, given that the selected access point satisfies other requirements (typically, BSSID, and WEP encryption) as well. The wireless client leaves or disassociates with the access point when the RSSI falls under a predefined threshold, such as when the user walks away from the coverage area of the access point. This association process, however, often results in uneven loads across access points, where many wireless clients are connected to only a few access points in a wireless environment, while other access points may remain idle or lightly loaded. That is, as discussed above, the wireless clients make association decisions based on what is best for the wireless client as opposed to what is best for the overall efficiency and performance of the wireless network environment.

As discussed above, the wireless client, therefore, acts only with regard to its own self-interest and, thus, will generally associate with the access point based on received signal strength without regard to the load on the access point (e.g., number of wireless clients, data throughput, etc.). The access point largely has no influence over the decision process at the wireless client except to deny the association requested by the wireless client. Denying the association, generally spurs the wireless client to repeat the process of discovering access points by transmitting probe requests and scanning the air for Beacon and Probe Response Frames. Many wireless clients, however, simply select the same access point as the logic the implement does not take account of previous association denials. Accordingly, this circumstance renders load balancing and other resource management tasks more problematic. In addition, even with wireless clients that take account of previous association denials, the discovery of access points by wireless client devices and having to repeat the process when associations are denied takes time, adversely affecting the operational efficiency of the network and degrading the wireless client user's experience.

The prior art for resource management in the area of wireless LANs addresses the problem of allocation of network resources by placing proprietary and non-standard intelligence in both the client and the access point in order to allow the client to make association decisions with information received from the radio access point. In order to be effective, it must limit the network to a homogenous client and infrastructure base, which typically is associated with proprietary software.

One example of such an infrastructure is found in I. Papanikos and M. Logothetis, A Study on Dynamic Load Balance for IEEE 802.11b Wireless LAN, cited as www.wcl.ee.upatras.gr/m-logo/papers/IEEE80211-P41.pdf, (7 pp.) and noted as posted as of at least 12 November 2002. This reference describes an algorithm in which the client makes an association decision based on: the number of clients associated with the radio access point, the received signal strength

indication (RSSI) value of the Probe Request received from the client by the radio access point, and the mean RSSI value of the signals received by the radio access point from other clients associated with the radio access point. The paper concludes that the algorithm does not perform well in the presence of hidden nodes and/or highly asymmetric traffic. Despite taking account of loading conditions, the association decisions are still allocated to the wireless client, which assesses a plurality of weighted factors to select an access point with which to associate. The association selection, however, may nevertheless not be appropriate based on the current loading conditions of the network. The selected access point in this instance will then deny the association request, causing the wireless client to repeat the scanning process.

In light of the foregoing, a need in the art for methods, apparatuses and systems that facilitate load balancing and other tasks associated with wireless network environments. A need further exists for a mechanism that reduces the number of association attempts in wireless computer networks. A need further exists for a mechanism that facilitates roaming in wireless network environments. Embodiments of the present invention substantially fulfill these needs.

SUMMARY OF THE INVENTION

The present invention provides methods, apparatuses and systems enabling a directed association mechanism in wireless computer network environments. In certain embodiments, the directed association functionality described herein can be used in a variety of contexts, such as directing wireless clients to associate with a particular access element or subset of access elements in a wireless network environment. In certain embodiments, the present invention can also be used to increase the efficiency of handing off wireless clients between access elements. As discussed below, the directed association mechanism, in one embodiment, increases the efficiency of establishing wireless connections between wireless clients and access points or elements in a wireless network system.

DESCRIPTION OF THE DRAWINGS

Figure 1 is a functional block diagram illustrating a wireless network system according to an embodiment of the present invention.

Figure 2 is a flow chart diagram providing a method enabling a directed association mechanism according to an embodiment of the present invention.

Figure 3 is a flow chart diagram providing a method, executed by a wireless client, enabling a directed association mechanism according to an embodiment of the present invention.

Figure 4 is a flow chart diagram setting forth a method, according to an embodiment of the present invention, enabling directed handoffs of wireless clients.

Figure 5 is a functional block diagram illustrating an alternative wireless network system architecture.

Figure 6 is a functional block diagram providing yet another alternative wireless network system architecture.

DESCRIPTION OF PREFERRED EMBODIMENT(S)

A. Network Environment Overview

For didactic purposes an embodiment of the present invention is described as operating in a WLAN environment as disclosed in U.S. application Ser. Nos. 10/155,938 and 10/407,357 incorporated by reference herein. As discussed below, however, the present invention can be implemented according to a vast array of embodiments, and can be applied to a variety of WLAN architectures.

Figure 1 illustrates a wireless computer network environment according to an embodiment of the present invention. Referring to Figure 1, there is shown a block diagram of a wireless Local Area Network system 10 according to an embodiment of the invention. A specific embodiment of the invention includes the following elements: access elements 12, 14 for wireless communication with selected client remote elements 16, 18, 20, 22, central control elements 24, 25, 26,

and means for communication between the access elements and the central control elements, typically direct line access 28, 30, but potentially a wireless backbone, fiber or other reliable link. As disclosed in U.S. patent application Ser. No. 10/407,357, in another embodiment, the access elements, such as access elements 12, 14 are directly connected to LAN 10 or a virtual local area network (VLAN) for communication with a corresponding central control element 24, 26. See Figure 5.

The access elements 12-15 are coupled via communication means using a wireless local area network (WLAN) protocol (e.g., IEEE 802.11a or 802.11b, etc.) to the client remote elements 16, 18, 20, 22. The communications means 28, 30 between the access elements 12, 14 and the central control element 24 is typically an Ethernet network, but it could be anything else which is appropriate to the environment. As described in U.S. Application Ser. Nos. 10/155,938 and 10/407,357, the access elements 12, 14 and the central control element 24 tunnel network traffic associated with corresponding remote client elements 16, 18; 20, 22 via direct access lines 28 and 30, respectively, or a LAN. Central control element 24 is also operative to bridge the network traffic between the remote client elements 16, 18; 20, 22 transmitted through the tunnel with corresponding access elements 12, 14.

In one embodiment, the access elements, such as access elements 12, 14, include functionality allowing for detection of the strength of the signal received from client remote elements and/or other access elements. For example, the IEEE 802.11 standard defines a mechanism by which RF energy is measured by the circuitry (e.g., chip set) on a wireless network adapter or interface card. The 802.11 protocol specifies an optional parameter, the receive signal strength indicator (RSSI). This parameter is a measure by the PHY layer of the energy observed at the antenna used to receive the current packet or frame. RSSI is measured between the beginning of the start frame delimiter (SFD) and the end of the PLCP header error check (HEC). This numeric value is typically an integer with an allowable range of 0-255 (a 1-byte value). Typically, 802.11 chip set vendors have

chosen not to actually measure 256 different signal levels. Accordingly, each vendor's 802.11-compliant adapter has a specific maximum RSSI value ("RSSI_Max"). Therefore, the RF energy level reported by a particular vendor's wireless network adapter will range between 0 and RSSI_Max. Resolving a given RSSI value reported by a given vendor's chip set to an actual power value (dBm) can be accomplished by reference to a conversion table. In addition, some wireless networking chip sets actually report received signal strength in dBm units, rather than or in addition to RSSI. Other attributes of the signal can also be used in combination with received signal strength or as an alternative. Again, many chip sets include functionality and corresponding APIs to allow for a determination of signal-to-noise ratios (SNRs) associated with packets received from client remote elements. In one embodiment, access elements 12, 14 include the detected signal strength and/or SNR value associated with a packet in the encapsulating headers used to tunnel the wireless packets to central control element 24. As discussed below, the remote client elements, in one embodiment, include signal attribute detection functionality as well.

As described in the above-identified patent applications, central control element 24 operates to perform data link layer management functions, such as authentication and association on behalf of access elements 12, 14. For example, the central control element 24 provides processing to dynamically configure a wireless Local Area Network of a system according to the invention while the access elements 12, 14 provide the acknowledgment of communications with the client remote elements 16, 18, 20, 22. The central control element 24 may for example process the wireless LAN management messages passed on from the client remote elements 16, 18; 20, 22 via the access elements 12, 14, such as authentication requests and authorization requests, whereas the access elements 12, 14 provide immediate acknowledgment of the communication of those messages without conventional processing thereof. Similarly, the central control element 24 may for example process physical layer information. Still further, the central

control element 24 may for example process information collected at the access elements 12, 14 on channel characteristic, propagation, and interference or noise. Central control elements 25, 26 and associated access elements 13, 15 operate in a similar or identical manner. Other system architectures are possible. For example, U.S. Application Ser. No. 10/407,357 discloses a system architecture where the access elements, such as access elements 12-15, are directly connected to LAN segment 10.

Other system architectures are also possible. For example, in another embodiment, the directed association functionality described herein can be implemented within the context of a single, autonomous access point, which can be configured to communicate with other access points and/or a central management platform 21 via SNMP, HTTP, or other protocols. See Figure 6.

B. Operation

As the following provides, the directed association functionality described herein can be used in a variety of contexts, such as directing wireless clients to associate with a desired access element or subset of access elements in a wireless network environment. In certain embodiments, the present invention can also be used to increase the efficiency of handing off wireless clients between access elements. These and other objectives will become apparent from the exemplary embodiment described below.

B.1. Directed Association

Figures 2 and 3 illustrate methods enabling the directed association mechanism according to an embodiment of the present invention. For didactic purposes, the embodiment described below is described as extensions to the 802.11 wireless communication protocol. As one skilled in the art will recognize, however, the present invention can be applied to any wireless network environment implementing any network communications protocol. As the following provides,

Figure 2 sets forth a method executed by an access point (such as a conventional access point, or an access element 12, 14 operating in connection with a central control element 24). Figure 3 illustrates a method executed by a wireless client, such as remote client element 16.

B.1.a. Wireless Client Functionality

As Figure 3 illustrates, upon start up or other event where a wireless client initializes a scan for access points with which to associate, the wireless client initializes variables and data fields associated with the scanning and directed authentication functionality described herein (202). For example, the wireless client may reset an association attempt counter to zero, or reset a table or list of detected access points or elements. The wireless client transmits Probe Requests and then scans its airspace on one to a plurality of operating channels for access points (204). In one embodiment, the wireless client scans all available channels in the region and listens to the Beacon or Probe Response Frames transmitted by access elements 12, 14, for example, in that region. The wireless client stores the RSSI (Received Signal Strength Indicator) of the Beacon or Probe Response Frames and other relevant information, such as BSSID, encryption (on/off), etc. After finishing the scan, the wireless client, in one embodiment, uses conventional processes to select an access element 12 or 14 with which to initially associate (206). For example, as discussed above, the wireless client can select the access element with the maximum RSSI, given that the selected access element covers other requirements (usually the BSSID, WEP encryption) as well. Of course, other selection algorithms can be used as well, whether or not involving extensions to the 802.11 or other applicable wireless protocol.

After selection of an access element, the wireless client transmits an association request (208) to the selected access element. In one embodiment, the wireless client includes a list of access elements (identified, in one embodiment, by MAC address and BSSID) detected during the scan. In one embodiment, the list is

embodied in a table which also includes the RSSI values detected during receipt of either Beacon or Probe Response Frames. In one embodiment, the list or table of access elements is ordered according to a preference computed by the wireless client. In 802.11 environments, the wireless client may first transmit an authentication request and receive an authentication response (not shown in Figures 2 or 3). As Figure 3 illustrates, the wireless client, in one embodiment, waits a threshold period of time for an association response from the selected access element (210). If no response is received, the wireless client repeats the process a configurable number (N) times (220, 222). If after N attempts, the selected access element does not respond, the wireless client reinitializes the access element scan.

If the access element responds, the wireless client determines whether the association response includes an acceptance notification or a rejection notification (212). If the access element accepts the requested association, the wireless client establishes or completes the wireless connection (214) according to the applicable wireless protocol. If the access element rejects the requested association, the wireless client scans the association response to determine whether it identifies alternative access elements with which to associate (see below). If so, the wireless client selects from the identified access element(s) and transmits an association request to the selected access element (218). As discussed in more detail below, generally speaking the newly requested association should be accepted as the list of alternative access elements was computed by the wireless network system as being available to the wireless client.

B.1.b. Access Element/Central Control Element Functionality

Figure 2 sets forth a method, according to an embodiment of the present invention, executed on the access point side of the wireless network environment. That is, the method described herein may be performed by an access element 12 operating in connection with a central control element 24, or by a conventional

access point architecture where the data link layer functions are not distributed between two components. See Figure 6. For didactic purposes, the embodiment described herein operates in a distributed, hierarchical wireless network environment including at least one central control element 24 and a plurality of access elements 12, 14, etc. Omitted from Figure 2 is a description of other data link layer functionality not immediately relevant to the present invention, such as the transmission of Beacon or Probe Response Frames by the access elements.

As Figure 2 provides, when an access element 12 receives an association request from a wireless client (102) it tunnels the association request to central control element 24. The central control element 24, in one embodiment, stores, in association with an identifier (e.g., MAC address) of the wireless client, a list of access elements that either detected the wireless client (e.g., by detecting a probe request) or a list of access elements detected by the wireless client provided in the association request (e.g., by receiving Beacon or Probe Response Frames during its scan) (104). More specifically, as discussed above, in one embodiment, the association request includes a list of access elements detected by the wireless client and may include other information such as RSSI or other signal related values (e.g., Signal-to-Noise Ratio, etc.). In another embodiment, the central control element 24 by virtue of managing other access elements, such as access element 14, and being able to communicate with other central control elements, such as central control element 26, can compile a list of access elements that detected the Probe Requests of the wireless client. This list can also be augmented to include additional information such as the RSSI or other signal attributes associated with the Probe Requests. In one embodiment, the central control elements 24, 25, 26 are configured with the computer network addresses (e.g., MAC address, IP address, etc.) of the other central control elements to exchange the wireless client identifiers of detected wireless clients, as well as which access element(s) detected the wireless clients. In one embodiment, the central control elements 24, 25, 26 maintain this information in a table or other suitable data structure and synchronize the data

structure with other central control elements as appropriate. In addition, the central control elements 24, 25, 26 can also monitor, and exchange with other central control elements, the load (e.g., number of clients, data throughput, duty cycle, etc.) associated with the access elements. Other load balancing or decisional criteria can include the other tasks an access element is called upon to perform, such as rogue access point detection, as disclosed in U.S. Application Ser. No. 10/407,370. In one embodiment, there is a central or master control element operative to perform the global load balancing computations for the entire wireless network system. In another embodiment, the central control elements are operative to synchronize load and other operational data with each other, such that each central control element can perform the load balancing or other decisional computations associated with identifying allowable access elements. In another embodiment, the wireless client can be configured to maintain its list of detected access elements locally and then compare its list to the list of allowable access elements returned in the association response in making its selection.

As Figure 2 shows, central control element 24 then computes a set of allowable access elements with which the wireless client can associate. The set of allowable access elements may be computed according to any suitable algorithm or process , incorporating various factors and criteria, configured to achieve a variety of objectives. For example, the set of allowable access elements may be computed according the load balancing functionality disclosed in U.S. Application Ser. No. 10/409,246. Other load balancing algorithms may also be used. In addition, the set of allowable access elements may be computed with regard to other factors, such as statically defined permissions based on wireless client MAC addresses, security policies, and the like. For example, wireless clients associated with guests or visitors to an enterprise may be forced to associate with only a subset of access elements. In other embodiments, the set of allowable access elements may be configured with respect to additional criteria, such as the duty cycle associated

with rogue access point detection or other tasks where a given access element goes off channel to perform a function.

In yet other embodiments, the list of allowable access elements may be computed with respect to geographic/location considerations, as well as detected radio-frequency connectivity or overlap among access elements. For example, as disclosed in U.S. Application Ser. No. 10/447,735, the access elements can be configured to exchange so-called neighbor messages to allow the central control elements or a central management platform to map the RF connectivity of the access elements. The set of allowable access elements can be reduced to the set of access elements having RF connectivity within a given signal strength threshold to the access element initially selected by the wireless client. In another embodiment, the central control elements can be configured with geographic or other location information relating to the access elements and select or further filter the set of allowable access elements based on geographic proximity to the access element initially selected by the wireless client.

In one embodiment, if the current access element 12 is included in the set of allowable access elements (108), then the central control element 24 sets the notification value in the association response to "accept" (110) and transmits the association response (118). Optionally, the association response may also include the set of other allowable access elements. However, if the current access element is not in the allowable set, the central control element 24 sets the notification value in the association response to "reject" (112). The central control element 24 then compares the set of access elements detected by (or detecting) the wireless client, see above, to the computed set of allowable access elements. If there is any overlap between the two sets, the central control element 24 appends the list of common access elements (in one embodiment, identified by MAC address) to the association response (116) and transmits the association response to the wireless client (118). As discussed above, the wireless client can then use this list of access elements in subsequent association attempts, being, in one embodiment, virtually guaranteed

(assuming the association request is transmitted in a sufficiently small period of time from the response) that an association request directed to an access element on this list will be accepted. As one skilled in the art will recognize, this protocol greatly reduces the time inherent in having to repeat the scan for access elements only to attempt to associate with the same access element, or another access element, that will deny the association.

In one embodiment, the table or other data structure included in the association response can include a variety of information. In one embodiment, the table can include the access element identifier, such as MAC address, and the BSSID of the access element. The table can also include other parameters, such as the operating channel of the access element, as well as operational parameters and characteristics, such as current load, and duty cycle. In one embodiment, the association response can also include other information, such as the RSSI values of the Probe Requests detected at each access element, to allow the wireless client to base its selection, at least in part, on this metric.

B.2. Directed Handoff

Once the wireless client is associated, the wireless network system, in one embodiment, can operate to facilitate handoffs of the wireless client between different access elements. For example, assume for didactic purposes that the data throughput load at access element 12 has risen above a threshold level, causing central control element 24 to decide that at least one currently-associated wireless client must be handed off to another access element.

Figure 4 illustrates a method enabling the directed handoff of the wireless client to another access element. In one embodiment, when the decision is made to initiate the handoff of a currently-associated wireless client, the central control element 24 first retrieves the list of access elements originally detected by the wireless client during the initial scan (see Section B.1., supra) (302). As above, the central control element 24 then computes a set of allowable access elements (304),

in one embodiment, by applying a load balancing algorithm, and compares the set of allowable access elements to the set of detected access elements (306). The central control element 24 appends the set of overlapping access element identifiers to a disassociation message (308) and transmits the disassociation message to the wireless client (310). As above, the wireless client can use the list of access element identifiers to select an access element and associate with the selected access element.

The invention has been explained with reference to specific embodiments. Other embodiments will be evident to those of ordinary skill in the art. For example, the present invention can also be applied to WLAN architectures beyond the hierarchical WLAN architecture described above. For example, in another embodiment, the directed association functionality described herein can be implemented within the context of a single, autonomous access point, which can be configured to exchange necessary information with other similarly configured access points and communicate with such access points over the wired network to coordinate configuration and other management tasks. See Figure 6. This distributed system of autonomous access points can be managed by a central network management platform 21 operative to distribute configuration information to the access points. In addition, although the embodiments described above, involve extensions to the 802.11 wireless networking protocol, the directed association mechanism can be applied to any suitable wireless network environment. It is, therefore, intended that the claims set forth below not be limited to the embodiments described above.